UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

7590 10/15/2007

David B Cochran
Jones Day Reavis & Pogue
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
10/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/594,368	LITTLE, HERB A.	
	Examiner	Art Unit	
	Tamara Teslovich	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on July 26, 2007 has been entered.

Claims 1, 16, and 31 are amended.

Claims 1-45 are pending and herein considered.

Response to Amendments and Arguments

Applicant's arguments filed July 26, 2007 have been fully considered but they are not persuasive.

Applicant's addition of the phrase "wherein the ephemeral key pair is used to encrypt a single plaintext message" to independent claims 1, 16, and 31 fails to overcome the Examiner's previously set forth 112 enablement and indefiniteness rejections. Although Applicant's remarks maintain that the addition of the above-mentioned limitation makes it clear that the key pair is only used for a limited time and "thereafter it is destroyed or deleted" such a conclusion does not flow directly from the claims as written. Instead of providing for the deletion of the keys, or a clear

explanation of how long they are to be used, Applicant's amendments specify that the ephemeral key pair is "used to encrypt a single plaintext message." Such a limitation is indefinite for two reasons. First, nowhere does Applicant provide for the deletion or destruction of the keys nor can his added limitation be taken as limiting any uses of the keys outside the encryption of messages. Whether or not Applicant intends to maintain the keys and use them for alternate purposes is unclear from the existing claim language. Secondly, Applicant's use of the phrase "used to encrypt a *single* plaintext message" calls into question how that same key pair can be used in subsequent steps to create digital signatures, signatures that by definition involve encryption of some kind or another, if that key pair may only be used to encrypt a *single* plaintext message. The Examiner has no choice but to maintain her 112 rejections of claims 1-45 until they are amended to clarify the extent and duration of the ephemeral key pair such that a person skilled in the art would be understand the point at which the ephemeral keys are to expire as ephemeral keys do. If it is the Applicant's intent to provide for an ephemeral key pair to be used for a single message transaction, that transaction including the encrypting of a plaintext message and the generation of a digital signature, all using the same ephemeral key pair, the Examiner requests that the Applicant make the amendments necessary.

The remaining 35 USC 112 issues mentioned above and further explained below render the claims indefinite, and as such the Examiner has no choice but to maintain her 35 USC 102 rejection of claims 1-45 in view of Schneier insofar as she understands

the reference to include those elements of the invention particularly claimed by the Applicant in his claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The Applicant's use of an "ephemeral key pair" more than once is non-enabling because the common technological use of "ephemeral key pairs' requires that they are created, used once, and destroyed immediately thereafter. Applicant's specification fails to clear up the issue insofar as the Applicant fails to provide for the destruction of the keys or even a suggestion as to the extent the keys are to be utilized. As the claims stand, it is unclear how many more times the ephemeral key pair can and will be used and whether or not they will ever expire.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "ephemeral key pair" in claims 1, 16, and 31 is used by the claim to mean "use more than once", while the accepted meaning is "use once and destroy." The term is indefinite because the specification does not clearly redefine the term. Applicant's specification fails to clear up the issue insofar as the Applicant fails to provide for the destruction of the keys or even a suggestion as to the extent the keys are to be utilized. As the claims stand, it is unclear how many more times the ephemeral key pair can and will be used and whether or not they will ever expire.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-45 remain rejected under 35 U.S.C. 102(e) as being anticipated by Schneier et al., US Pat 5,956,404.

Regarding **Claims 1, 16, and 31**, Schneier teaches a public-key encryption process and system comprising the steps of a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message (see Schneier col.1 lines 28-44) wherein the ephemeral key pair is used to encrypt a single plaintext message; and b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step (see Schneier col.1 lines 45-65).

Regarding **Claims 2, 17, and 32**, Schneier teaches a public-key encryption process and system wherein the encrypting step uses an El Gamal encryption scheme (see Schneier col.1 lines 45-65).

Regarding **Claim 3**, Schneier teaches a public-key encryption process wherein the step of generating a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme; wherein the step of generating the digital signature includes hashing the plaintext message (see Schneier col.1 lines 45-65).

Regarding **Claims 18, and 33**, Schneier teaches a public-key encryption process and system wherein the step of generating a digital signature comprises generating the

digital signature using a Nyberg-Rueppel digital signature scheme (see Schneier col.1 lines 45-65).

Regarding **Claims 4, 19, and 34**, Schneier teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG, where G is a generator (see Schneier col.1 lines 28-44).

Regarding **Claims 5, 20, and 35**, Schneier teaches a public-key encryption process and system for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key A = aG, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key B = bG,

wherein the sender obtains an authentic copy of the receiver public key B and the receiver obtains an authentic copy of the sender public key A (see Schneier col.1 lines 28-44).

Regarding **Claims 6, 21, and 36**, Schneier teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises

the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG (see Schneier col.1 lines 28-44).

Regarding **Claims 7, 22, and 37**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the sender, generating a secret key K = xB and encrypting a plaintext message using the secret key K to generate a ciphertext message (see Schneier col.1 lines 28-44).

Regarding **Claims 8, 23, and 38**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature (see Schneier col.1 lines 45-65).

Regarding **Claims 9, 24 and 39**, Schneier teaches a public-key encryption process and system, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver (see Schneier col.1 lines 45-65).

Regarding **Claims 10, 25, and 40**, Schneier teaches a public-key encryption process and system, further comprising the steps of, at the receiver, generating the secret key K = bX = bxG = xbG = xB, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital signature using the decrypted message and the transmitted encryption ephemeral public key X

and validating the digital signature based on the calculated first value r and the transmitted second value s (see Schneier col.1 lines 45-65).

Regarding **Claim 11**, Schneier teaches a the public-key encryption process of Claim 1, wherein at least a two-stage public-key encryption process is used; wherein the first stage includes key establishment and the second stage includes encryption/decryption; wherein said steps (a) and (b) are performed during the second stage of encryption (see Schneier col.1 lines 45-65).

Regarding **Claims 12-15, 26-30 and 41-45**, Schneier teaches a public-key encryption process and system and its implementation in wireless hand-held communication devices within a communication system (see Schneier col.5 lines 8-40).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

T. Teslovich

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER